REMARKS

[0001] Applicant respectfully requests entry of the following remarks and reconsideration of the subject application. Applicant respectfully requests entry of the amendments herein. The remarks and amendments should be entered under 37 C.F.R. §1.116 as they place the application in better form for appeal, or for resolution on the merits.

[0002] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-6, 10-15, 18, and 28-29 are presently pending. Claims amended herein are: 1, 12-13, 18 and 28-29. Claims cancelled herein are: 7-9, 16-17, 19-27 and 30-31. No new claims are added herein.

Formal Request for an Interview

[0003] If the Examiner's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0004] Please contact me or my assistant to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for us, I welcome your call to either of us as well. Our contact information may be found on the last page of this response.

Claim Amendments

[0005] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 1, 12-13, 18 and 28-29 herein.

Formal Matters

[0006] This section addresses any formal matters (e.g., objections) raised by the Examiner.

Claims

[0007] The Examiner objects to claims 13-15 and 18 for reciting "a employer" instead of "an employer". Herein, Applicant amends these claims, as shown above, to correct the informalities noted by the Examiner.

Substantive Matters

Claim Rejections under §112 1ST ¶

[0008] Claims 1-6, 10-15, and 18 are rejected under 35 U.S.C. §112, 1st ¶ for reciting "when" instead of "after". In light of the amendments presented herein, Applicant submits that these rejections are moot. Accordingly, Applicant asks the Examiner to withdraw these rejections.

Claim Rejections under §101

[0009] Claims 12, 18, and 28-29 are rejected under 35 U.S.C. §101. In light of the amendments presented herein, Applicant respectfully submits that these claims comply with the patentability requirements of §101 and that the §101 rejections should be withdrawn. The Applicant further asserts that these claims are allowable. Accordingly, Applicant asks the Examiner to withdraw these rejections.

[0010] If the Examiner maintains the rejection of these claims, then the Applicant requests additional guidance as to what is necessary to overcome the rejection.

Claim Rejections under § 103

[0011] The Examiner rejects claims 1-6, 10-15, 18, and 28-29 under §103. For the reasons set forth below, the Examiner has not made a prima facie case showing that the rejected claims are obvious.

[0012] Accordingly, Applicant respectfully requests that the §103 rejections be withdrawn and the case be passed along to issuance.

[0013] The Examiner's rejections are based upon the following reference in view of Examiner's Official Notice:

- **Gatz:** *Gatz, et al.,* US Patent Publication No. 2002/0049806 (published April 25, 2002).

Overview of the Application

[0014] The Application describes a technology for identifying a permission level associated with a child's access to a Web server. A relationship ticket is obtained from an authentication server and a request is generated to set the identified permission level. The request and the relationship ticket are sent to the Web server and a success code is received from the Web server if the requested permission level is established. (see Application, Abstract)

Cited References

[0015] The Examiner cites Gatz as the primary reference in the obviousness-based rejections.

Gatz

[0016] Gatz describes a technology for an access server that controls use of services in an account based access server and includes a database of users, a data structure associating users identified as parents with parent accounts, users

identified as children with child accounts and associating parent accounts with child accounts in family accounts. The access server includes logic for verifying parental status of a parent account with respect to a child account and logic for limiting access to a user using a child account that is associated with a family account, where such limitations are determined, at least in part, based on selections made by a user of a parent account associated with the family account. (*Gatz*, Abstract)

Obviousness Rejections

Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

[0017] Applicant disagrees with the Examiner's obviousness rejections. Arguments presented herein point to various aspects of the record to demonstrate that all of the criteria set forth for making a prima facie case have not been met.

Based upon Gatz

[0018] The Examiner rejects claims 1-6, 10-15, 18, and 28-29 under 35 U.S.C. § 103(a) as being unpatentable over Gatz in view of Examiner's official notice. Applicant respectfully traverses the rejection of these claims and asks the Examiner to withdraw the rejection of these claims.

Independent Claim 1

[0019] Applicant submits that Gatz (alone or in combination with any other cited reference) does not render this claim unpatentable because they do not show, teach or suggest at least the following features as recited in this claim (emphasis added):

- communicating--*by a parent using a client device*--a parental identity to an authentication server for verification
- receiving a relationship ticket from the authentication server after the parental identity has been successfully verified, wherein the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by the *client device which receives the relationship ticket*, and wherein the relationship ticket includes the parental identity and identifies a child who's access to a Web server is to be limited;
- generating–by the parent using the client device--a request to establish a selected permission level for the child which will limit the child's access to the Web server;
- *sending--by the parent using the client device--the request and the relationship ticket to the Web server* for:
    - decryption of the relationship ticket;
    - performing an integrity check of the relationship ticket using a message authentication code contained within the relationship ticket;
    - *authentication of the parental identity*, , wherein the Web server authenticates the parental identity with the authentication server using the contents of the relationship ticket; and
    - establishment of the selected permission level for the child;
- receiving--by the *client device--a success code* from the Web server if the selected permission level is established for the child

[0020] The Examiner indicates (Action, p. 5-7) the following with regard to this claim:

As per **claim 1**, Gatz et al. discloses a method comprising:

Communicating a parental identity to an authentication server for verification (par. [0063]);

Receiving a relationship ticket from the authentication server when the parental identity has been successfully verified (e.g. abstract, paragraph [0015], Fig. 3 and Fig. 4) and wherein the relationship ticket includes the parental identity and identifies a child who's access to a Web server is to be limited (e.g. par. [0064]);

Generating a request to establish a selected permission level for the child which will limit the child's access to the Web server (e.g. paragraph [0058], [0060] and [0066]-[0069]);

authentication of the parental identity, and establishment of the selected permission level for the child (e.g. fig. 12, paragraph [0069] and [0071]); and

receiving a success code from the Web server if the selected permission level is established (e.g. paragraph [0070]).

Gatz et al. does not expressly disclose wherein the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by a client device which receives the relationship ticket and Sending the request and the relationship ticket to the Web server for decryption of the relationship ticket. However, the examiner takes official notice that the above missing features from Gatz et al. are well known in the art to a person with ordinary skill in the art. For example, at the time of the invention, AOL and other web navigation companies such as Yahoo, Excite, MSN, Microsoft, Google already had this well known feature in the systems to enhance parental/employer control. It would have been obvious to a person with ordinary skill in the art to incorporate this well known feature to the Gatz et

al.'s method to enhance the parental/employer control to access web sites, e-mails and etc in order to produce predictable results.

[0021] Applicant traverses the Examiner's assertion of Official Notice for reasons provided below, and asks the Examiner for an affidavit to support Examiner's assertion of Official Notice.

[0022] For example, Gatz (alone or in combination with any other cited reference) does not show, teach or suggest "receiving a relationship ticket from the authentication server after the parental identity has been successfully verified, wherein the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by the *client device which receives the relationship ticket*, and wherein the relationship ticket includes the *parental identity* and *identifies a child* who's access to a Web server is to be limited" and "*sending--by the parent using the client device--the request and the relationship ticket to the Web server* for: decryption of the relationship ticket; performing an integrity check of the relationship ticket using a message authentication code contained within the relationship ticket; *authentication of the parental* identity wherein the Web server authenticates the parental identity with the authentication server *using the contents of the relationship ticket*; and establishment of the selected permission level for the child" as recited in this claim.

[0023] As evidenced above (Action p. 6-7), the Examiner states that Gatz et al. does not disclose wherein the relationship ticket is encrypted or decrypted, and the Examiner takes official notice that the above missing features from Gatz

are well known in the art to a person with ordinary skill in the art [at the time of the invention] and is a well known feature in systems used to enhance parental/employer control. Applicant respectfully disagrees. Furthermore, Applicant traverses the Examiner's assertion of Official Notice (see M.P.E.P. 2144.03) and asks the Examiner for an affidavit to support Examiner's assertion of Official Notice. Applicant contends that the Examiner has not addressed all features of the *relationship ticket* as recited in this claim. Applicant requests that the Examiner provide prior art evidence showing at least the following elements and features recited in this claim:

- "receiving a relationship ticket from the authentication server after the parental identity has been successfully verified"
- "the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by a client device which receives the relationship ticket"
- "the relationship ticket includes the parental identity and identifies a child who's access to a Web server is to be limited"
- "sending--by the parent using client device--the request and the relationship ticket to the Web server for: decryption of the relationship ticket; performing an integrity check of the relationship ticket using a message authentication code contained within the relationship ticket; *authentication of the parental* identity wherein the *Web server authenticates the parental identity with the authentication server using the contents of the relationship ticket;*"

[0024] With regard to "receiving a relationship ticket from the authentication server after the parental identity has been successfully verified ...

the client device which receives the relationship ticket", the Examiner equates these claim features with Gatz abstract, ¶ [0015] and figures 3-4. Applicant respectfully disagrees.

[0025] For example, Gatz states the following:

> The access server includes logic for verifying parental status of a parent account with respect to a child account and logic for limiting access to a user using a child account that is associated with a family account, where such limitations are determined, at least in part, based on selections made by a user of a parent account associated with the family account (see *Gatz*, Abstract and ¶ [0015]).

[0026] Figures 3 and 4 of Gatz represents data in a database in the access server system representing relationships between family, parent, and child accounts as well as family preferences (i.e., limitations on child account access privileges).

[0027] Gatz (alone or in combination) does not show, teach or suggest "receiving a relationship ticket from the ***authentication server*** after the parental identity has been successfully verified ... *the client device which receives the relationship ticket*" because, as evidenced above, data defining relationships between parents and children are maintained in the access system database (Gatz, figure 3-4), and the access server includes logic for verifying parental status of a parent account with respect to a child account (see *Gatz*, Abstract and ¶ [0015]). This would imply that the access server equates to the Applicant's "authentication server".

[0028] Gatz (alone or in combination) does not show, teach or suggest "*sending--by the parent using the client device--the request and the relationship ticket to the* ***Web server*** for: decryption of the relationship ticket ... *authentication of the parental identity*, wherein the Web server authenticates the parental identity with the authentication server *using the contents of the relationship ticket*" because data defining relationships between parents and children are maintained in the access system database (Gatz, figure 3-4), and the access server includes logic for verifying parental status of a parent account with respect to a child account (see *Gatz*, Abstract and ¶ [0015]). This would imply that the access server equates to the Applicant's "Web server".

[0029] In light of Gatz (alone or in combination), the combination of "receiving a relationship ticket from the authentication server" and "*sending--by the parent using the client device--the request and the relationship ticket to the Web server*" described above makes no sense, because it would equate to the parent receiving encrypted user account information (that the parent can not decrypt) from the access server and then sending it back to the access server for decryption and verification. There would be no rationale for Gatz (alone or in combination) to perform this "receiving" and "sending".

[0030] Furthermore, with regard to "receiving--by the parent using the client device--a success code from the Web server if the selected permission level is established for the child" the Examiner cites Gatz, which teaches that when a parent changes a child's password, the access system will send the affected ***child*** and associated ***child account*** an email confirmation (Gatz, ¶ [0070]). In contrast, this claim recites "receiving--by the parent using the client device--a

success code from the Web server" which is not analogous to the ***child*** receiving any confirmation.

[0031] Consequently, Gatz (alone or in combination) does not disclose all of the claimed elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claim 5

[0032] Claim 5 depends from claim 1. Applicant submits that Gatz (alone or in combination) does not render this claim unpatentable because they do not show, teach or suggest at least the following features as recited in this claim (emphasis added):

> A method as recited in claim 1 wherein the *relationship ticket is encrypted by the authentication server.*

[0033] The Examiner indicates (Action, p. 5-7) the following with regard to this claim:

> As per **claim 5**, Gatz et al. – examiner's official notice discloses a method as applied above in **claim 1**. Gatz et al. further discloses wherein the relationship ticket is encrypted by the authentication server ("...the user might select to verify account control requirements 92 over a secure network connection using, for example, SSL (Secure Socket Layer) or the like" – e.g. paragraph [0062]. Please note to a person in the ordinary skill in the art that SSL uses cryptographic system that uses two keys to encrypt data)

[0034] SSL is a protocol for transmitting private documents via the Internet, and SSL uses two keys to encrypt data: (1) a public key known to everyone, and (2) a private key known only to the recipient of the message. However, claim 1 recites that "the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by a client device which receives the relationship ticket". Dependent claim 5 recites that "the

relationship ticket is encrypted by the authentication server". In contrast, according to the SSL protocol, the recipient of the message has a private key to decrypt the message. Accordingly, Gatz (alone or in combination) also does not show or disclose that "the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by the client device which receives the relationship ticket", as recited in claim 1 (emphasis added).

[0035] Furthermore, the Application states:

> Various types of information in different formats (such as tickets or tokens) can be utilized with the systems and methods discussed herein. The systems and methods described herein do not require the use of secure communication protocols such as SSL (Secure Sockets Layer). (*Application*, page 4, lines 6-9)

[0036] Consequently, Gatz (alone or in combination) does not disclose all of the claimed elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Independent Claim 13

[0037] Applicant submits that Gatz (alone or in combination) does not render this claim unpatentable because they do not show, teach or suggest at least the following features as recited in this claim (emphasis added):

- communicating—by *an employer using a client device*--an employer identity to an authentication server for verification
- receiving a relationship ticket from the authentication server after the employer identity has been successfully verified, wherein the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by a *client device which receives the relationship ticket*, and wherein the relationship ticket includes the employer identity and identifies an employee who's access to a Web server is to be limited;
- generating a request to establish a selected permission level for the employee which will limit the employee's access to the Web server;
- sending--by a *client device*-- the request and the relationship ticket to the *Web server for decryption of the relationship ticket, authentication of the employer identity, and establishment of the selected permission level for the employee*;
- receiving--by a *client device-- a success code from the Web server* if the selected permission level is established for the employee

[0038] For example, Gatz (alone or in combination) does not show, teach or suggest "receiving a relationship ticket from the authentication server after the employer identity has been successfully verified, wherein the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by a *client device which receives the relationship*

ticket, and wherein the relationship ticket includes the employer identity and identifies an employee who's access to a Web server is to be limited" and "sending--by a *client device*--the request and the relationship ticket to the *Web server for decryption of the relationship ticket, authentication of the employer identity, and establishment of the selected permission level for the employee*" as recited in this claim.

[0039] As discussed above regarding independent claim 1, Applicant contends that the Examiner has not addressed all features of the *relationship ticket* as recited in this claim. Furthermore, Applicant traverses the Examiner's assertion of Official Notice (see M.P.E.P. 2144.03) and asks the Examiner for an affidavit to support Examiner's assertion of Official Notice. Applicant requests that the Examiner provide prior art evidence showing at least the following elements and features recited in this claim:

- "receiving a relationship ticket from the authentication server after the employer identity has been successfully verified"
- "the relationship ticket received from the authentication server is encrypted so that the relationship ticket cannot be decrypted by a client device which receives the relationship ticket"
- "the relationship ticket includes the employer identity and identifies an employee who's access to a Web server is to be limited"
- "sending--by a client device-- the request and the relationship ticket to the Web server for decryption of the relationship ticket"

- "sending--by a client device-- the request and the relationship ticket to the Web server for decryption of the relationship ticket, authentication of the employer identity"

[0040] As also discussed above for claim 1, the combination of "receiving a relationship ticket from the authentication server" and "*sending--by the client device--the request and the relationship ticket to the Web server*" described above makes no sense, because it would equate to receiving user account information from the access server and then sending it back to the access server for verification. There would be no rationale for Gatz (alone or in combination) to perform this "receiving" and "sending".

[0041] Furthermore, with regard to "receiving--by the client device--a success code from the Web server if the selected permission level is established for the employee" the Examiner cites Gatz, which teaches that when a parent [employer] changes a child's [employee's] password, the access system will send the affected ***child*** and associated ***child account*** an email confirmation (Gatz, ¶ [0070]). In contrast, this claim recites "an *employer* using a client device" which is not analogous to the ***child*** [employee] receiving a confirmation.

[0042] Consequently, the combination of Gatz (alone or in combination) does not disclose all of the claimed elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Independent Claim 28

[0043] Applicant submits that Gatz (alone or in combination) does not render this claim unpatentable because they do not show, teach or suggest at least the following features as recited in this claim (emphasis added):

- select–*by a manager's client device--a permission level* associated with an associate's access to a Web server;
- obtain–*by the manager's client device*--a relationship ticket from an authentication server, wherein the *relationship ticket* obtained from the authentication server is encrypted and includes *information regarding a manager's identity and information regarding an identity of an associate who's access to the Web server is to be limited*;
- generate a request to establish a selected permission level for the associate which will limit the associate's access to the Web server;
- send–*by the manager's client device*--the request and the relationship ticket *to the Web server* via an unsecure communication link for decryption of the relationship ticket, *authentication of the manager's identity, and establishment of the selected permission level for the associate*;
- *receive–by the manager's client device-- a success code from the Web server* if the requested permission level is established for the associate

[0044] For example, Gatz (alone or in combination) does not show, teach or suggest "obtain–*by the manager's client device*--a relationship ticket from an authentication server, wherein the *relationship ticket* obtained from the authentication server is encrypted and includes *information regarding a manager's identity and information regarding an identity of an associate who's*

access to the Web server is to be limited" and "send–*by the manager's client device*--the request and the relationship ticket *to the Web server* via an unsecure communication link for decryption of the relationship ticket, *authentication of the manager's identity, and establishment of the selected permission level for the associate*" as recited in this claim.

[0045] As discussed above regarding independent claim 1, Applicant contends that the Examiner has not addressed all features of the *relationship ticket* as recited in this claim. Furthermore, Applicant traverses the Examiner's assertion of Official Notice (see M.P.E.P. 2144.03) and asks the Examiner for an affidavit to support Examiner's assertion of Official Notice. Applicant requests that the Examiner provide prior art evidence showing at least the following elements and features recited in this claim:

- "obtain–by the manager's client device--a relationship ticket from an authentication server, wherein the relationship ticket obtained from the authentication server is encrypted and includes information regarding a manager's identity and information regarding an identity of an associate who's access to the Web server is to be limited"
- "send–by the manager's client device--the request and the relationship ticket to the Web server via an unsecure communication link for decryption of the relationship ticket, authentication of the manager's identity, and establishment of the selected permission level for the associate"

[0046] As also discussed above for claim 1, the combination of "obtain–by the manager's client device--a relationship ticket from an authentication server" and "send–by the manager's client device--the request and the relationship ticket

to the Web server" described above makes no sense, because it would equate to receiving user account information from the access server and then sending it back to the access server for verification. There would be no rationale for Gatz (alone or in combination) to perform this "receiving" and "sending".

[0047] Furthermore, with regard to "receive–by the manager's client device--a success code from the Web server if the requested permission level is established for the associate" the Examiner cites Gatz, which teaches that when a parent [manager] changes a child's [associate's] password, the access system will send the affected ***child*** and associated ***child account*** an email confirmation (Gatz, ¶ [0070]). In contrast, this claim recites "receive–by the manager's client device" which is not analogous to the ***child*** [associate] receiving a confirmation.

[0048] Consequently, the combination of Gatz (alone or in combination) does not disclose all of the claimed elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims

[0049] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0050] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call/email me or my assistant at your convenience.

Respectfully Submitted,

Dated: 5-5-2009

By: E. John Fain

E. John Fain
Reg. No. 60960
(509) 324-9256 x256
johnf@leehayes.com
www.leehayes.com

My Assistant: Megan Arnold
(509) 324-9256 x270
megan@leehayes.com